



STANDARD OPERATING PROCEDURES

Wisconsin Department of Commerce
Division of Community Development

Bureau of Housing

201 West Washington, 5th Floor

P.O. Box 7970

Madison, WI 55707-7970

sphelp@commerce.state.wi.us



Table of Contents

Introduction	I
Contacts	III
Requirements For Participation	1
Technological Requirements	1.1
Participation Requirements	1.2
Initial And Annual Fee Structure For Wisp Licenses	1.3
Confidentiality and Security (Controls and Limits)	2
Confidentiality and Informed Consent	2.1
Confidential Data	2.2
Data Assessment and Access	2.4
Bowman Internet Systems	2.5
DOA – System Administrators	2.6
Virtual Private Network (VPN)	2.7
Partner Agencies	2.8
Access Privileges to System Software	2.9
Access Levels for System Users	2.10
Anonymous Clients	2.11
ROI	2.12
Data Expectation (Output)	3
Data Collection Protocol	3.1
Assessment Setup	3.2
Data Integrity and Reliability	3.3
Default Restrictions and Exceptions	3.4

INTRODUCTION

The Wisconsin ServicePoint (WISP) Project is the statewide implementation of a Homeless, Management Information System (HMIS) and is administered by the Department of Commerce, Division of Community Development – Bureau of Housing and Bowman Internet Systems. Bowman Internet Systems administers the central server and Commerce administers licensing, training and compliance. The project utilizes Internet-based technology to assist homeless service organizations across Wisconsin in capturing information about the clients that they serve.

Goals of WISP are to enable service providers to measure the effectiveness of their interventions, facilitate longitudinal analysis within continuums of care (CoC) of service needs and gaps, therein informing public policy about the extent and nature of homelessness in the state of Wisconsin. This is accomplished through analysis and release of data that are grounded in the actual experiences of homeless persons and the service providers who assist them in shelters and homeless assistance programs throughout the state.

Benefits Accrued through WISP:

For Service Providers

Provides online real-time information about needs and available services for homeless persons

Assures confidentiality by providing information in a secured system;

Decreases duplicative client intakes and assessments;

Tracks client outcomes and provides a client history;

Generates data reports for local use and to meet state and federal reporting requirements;

Facilitates the coordination of services internally and externally with other agencies and programs;

Provides access to a statewide database of service providers and allows agency staff to easily select a referral agency.

For Homeless Persons

Intake information and needs assessments are maintained historically so the number of times homeless persons must repeat their stories to multiple service providers is reduced.

The opportunity to provide intake and life history one time demonstrates that service providers consider the homeless person's time is valuable and restores some of the consumer's dignity.

Multiple services can be easily coordinated and referrals streamlined; and

For the State of Wisconsin

Better able to define and understand the extent of homelessness throughout Wisconsin;

Better able to focus staff and financial resources to those geographical areas, agencies and programs where services for homeless persons is needed the most;

Better able to evaluate the effectiveness of specific interventions and specific programs and services provided.

Better able to provide the State Legislature and the federal government with data and information on the homeless population in Wisconsin; and

Better able to meet all federal reporting requirements.

made available to policy makers, service providers, advocates, and consumer representatives. The WISP project is advised by a broad-based steering committee committed to understanding the gaps in services to consumers of the human service delivery system in an attempt to end homelessness.

Involvement in the project provides the capacity to programs within a CoC to generate automated APRs, to access aggregate reports that can assist in completion of the HUD-required gaps chart and consolidated plans, and to utilize the aggregate data to inform policy decisions aimed at addressing and ending homelessness at local, state and federal levels.

This document provides the policies, procedures, guidelines, and standards that govern WISP operations, as well as roles and responsibilities for Bowman Internet Systems and participating agency staff. Participating agencies will receive all relevant portions of the complete document, with the exception of those procedures that, if disseminated, would compromise the underlying security features of the Central Server and overall system.

CONTACTS

To contact any of the BOH staff or steering committee members listed below, please e-mail sphelp@commerce.state.wi.us. Within the e-mail make sure to indicate whom you would like to speak with.

❖ **Bureau of Housing – Wisconsin Department of Commerce**

Phil Wells – WISP Budget, Policy and Program Management–

- Sets overall policy and project direction
- Manages budgets
- Oversees the work break down on tasks associated with the WISP project
- Acts as the contact for the business end of Bowman Systems and as the policy contact with HUD

Loren Hoffmann – WISP IT and Report Coordination —

- Deals with technological issues in WISP
- Manages data migration and conversion issues with new agencies
- Reports out the statics for the HMIS for both policy and data quality issues
- Develops custom reports upon request from partner agencies
- Maintains WISP's Web Page
- Acts as the contact for the State with Bowman Systems on matters related to the database programming, reporting and user interface

Tanya Wagner – WISP Customer Services and Training –

- Manages WISP HelpDesk
- Develops support material
- Trains users and administrators on WISP
- Assists with data quality issues
- Acts as the contact for users of the software from the participating agencies

Don Hammes – WISP Billing and Contract Compliance—

- Invoices WISP Partner Agencies for their continuing and new licenses
- Ensures that proper documentation is filled out and filed on all WISP partner agencies
- Acts as the contact for new agencies interested in becoming a WISP partner
- Publishes the WISP Newsletter

❖ **State of Wisconsin HMIS Steering Committee**

Name	Agency	City / County
Linda Shaw	Community Referral Agency	Milton / Polk
Mike Fatica	ENTECH *	Statewide
Jennifer Allen	Forward Service Corporation	Green Bay / Brown
Patti Abbot	Hope House	Milwaukee / Milwaukee
Adam Smith	Porchlight	Madison / Dane
Aubre Wellens	Shalom Center	Kenosha / Kenosha
Kathie Walker	SDC / Milwaukee CoC**	Milwaukee / Milwaukee
Mary ClaySantineau	Starting Points	Chippewa Falls / Chippewa
Karen Smith	Western Dairyland	Independence / Trempealeau
Vicki Berenson	WCADV***	Statewide
Joana Hemschemeyer	Waukesha Housing Authority	Waukesha / Waukesha
Faith Holley-Beal	The Women's Center	Waukesha / Waukesha

Participation Requirements

Section 1

TECHNOLOGICAL REQUIREMENTS

Policy: WISP staff will establish requirements for participation. All requirements for participation are outlined in this Standard Operating Procedure manual.

The Minimum Workstation Recommendations

- Pentium Class PC
- 128 MB RAM
- Microsoft Internet Explorer 5.5 or higher, or Netscape Navigator 6 + (It is recommended that your browser have a 128 cipher / encryption strength installed. The browser's cache should be set to "Check for new version of the stored pages: Every visit to page.")
- Broadband Internet connection (hosted version) or LAN connection.
- Virus protection updates

Bandwidth Recommendations

- The average user will need to sustain a 30-50 Kilo Bytes/ Sec of download throughput to comfortably browse the Wisconsin ServicePoint Web Site.
- Internet Bandwidth Comparisons
 - ✓ **56K Modem** – Most users will achieve a connection between 26.4K – 46K connection depending upon the phone line quality. This will provide at least a 5.0 KB/S transfer rate which is low and not recommended for a single user.
 - ✓ **SDSL** – 512Kbps/62.5KB/s. Allows eight users to concurrently browse Wisconsin ServicePoint or use the Internet.
 - ✓ **ADSL** – 1.5-8Mbps/187.5KB/s-1MB/s. Allows 23 – 125 users concurrently to use Wisconsin ServicePoint or use the Internet. Distance limited to 18,000 feet.
 - ✓ **Cable** – 1Mbps/122.1KB/s. Allows 15 users to concurrently use Wisconsin ServicePoint or the Internet.
 - ✓ **T1** – 1.544Mbps/188.5KB/s. Allows 23 users to concurrently use Wisconsin ServicePoint or the Internet.
 - ✓ **T3** – 44.763Mbs/5.461MB/s. Allows 682 users to concurrently use ServicePoint or the Internet.

PARTICIPATION REQUIREMENTS

Policy:	WISP staff will establish requirements for participation. All requirements for participation are outlined in this Standard Operating Procedure manual.
----------------	--

Procedure:

Identification of Agency Administrator: Designation of one or more key staff to serve as the agency administrator. This person will be responsible for creating usernames and passwords and monitoring software access. This person will also be responsible for training new agency staff persons on how to use the WISP.

Training: Commitment of site Agency Administrators and designated staff persons to attend training(s) prior to accessing the system online. If the Agency Administrator changes, then the new administrator must attend a training.

Client Consent Forms: These must be signed by clients to authorize the sharing of their personal information electronically with other participating agencies through the WISP where applicable.

Data Protocols: Agencies must identify which data elements they wish to collect in addition to the minimally required data elements established by the WISP Steering Committee in accordance with HUD.

Participation Agreement: Agencies are required to sign a participation agreement stating their commitment to adhere to the policies and procedures for effective use of the system and proper collaboration with WISP.

INITIAL AND ANNUAL FEE STRUCTURE FOR WISP LICENSES

Policy: Bureau of Housing staff will establish both initial start-up and annual continuance fee requirements for participation in WISP. This policy will be set at a rate that maximizes the State's ability to meet its match requirement and still be affordable to agencies. The fee structure seeks to maximize scale economies with a diminishing marginal cost.

Procedure:

Initial Start-up Fees

The fee for the license is the cost required to add an individual to the system. The first couple users added to the system have higher marginal costs than the fourteenth user and the fee structure reflects this. The tiers for the fees are as follows:

1st User	<i>Tier 1</i>	6th – 10th User	<i>Tier 4</i>
2nd User	<i>Tier 2</i>	11th – ∞	<i>Tier 5</i>
3rd – 5th User	<i>Tier 3</i>		

Example If an agency wishes to buy four user licenses, then the fee would be structured such that the first licenses would be from *Tier 1*, the second from *Tier 2*, and the third and fourth from *Tier 3*. If the following year that same agency wanted to buy another two user licenses then the fee would be structured that the fifth license would be from *Tier 3* and the sixth would be from *Tier 4*.

To see the fee associated with each tier go to the Licensing Fee Chart. Fees are subject to change from one fiscal year to the next.

Annual Continuance Fee

In each year, each WISP partner agency will be charged a percentage of their initial licensing fee to continuing using the system and the support from the Bureau of Housing. This fee is subject to change for each fiscal year, the percentage rate charged in any given fiscal year is in the licensing fee chart.

If an agency reduces the number of WISP licenses, the initial fee will not be returned but the annual percentage fee will be calculated against the total license fee minus the original cost for the licenses that are returned.

Confidentiality and Security

Section 2

Confidentiality and Informed Consent	2.1
Open and Confidential Data– System Administration	2.2
Open and Confidential Data– Partner Agency	2.3
Data Assessment and Access	2.4
owman Internet Systems	2.5
DOA – System Administrators	2.6
Virtual Private Network (VPN)	2.7
Partner Agencies	2.8
Access Privileges to System Software	2.9
Access Levels for System Users	2.10
Anonymous Clients	2.11
ROI	2.12

CONFIDENTIALITY AND INFORMED CONSENT

Policy:	The agency shall uphold relevant federal and state confidentiality regulations and laws that protect Client records and only release client records with written consent by the client, unless otherwise provided for in the regulations. For a list of these regulations and laws, please see Appendix B .
----------------	--

Procedure: Participating Agencies are required to develop procedures for providing oral explanations to clients about the usage of WISP. This is called informed consent. Agencies are required to use written client consent forms when information is to be shared with another agency to ensure protection of clients' privacy. The Agency agrees not to release any confidential information received from the WISP database to any organization or individual without proper written consent

Informed Consent:

Oral Explanation (non-shared records): All clients will be provided an oral explanation that their information will be entered into a computerized record keeping system. The Partner Agency will provide an oral explanation of the WISP project and the terms of consent. The agency is responsible for ensuring that this procedure takes place at the initial interview for every client. The document must contain the following information:

- 1. What Wisconsin ServicePoint is**
 - Web based information system that homeless services agencies across the state use to capture information about the persons they serve
- 2. Why the agency uses it**
 - To understand their clients' needs
 - Help the programs plan to have appropriate resources for the people they serve
 - To inform public policy in an attempt to end homelessness
- 3. Security**
 - Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records
- 4. Privacy Protection**
 - No information will be released to another agency without written consent
 - Client has the right to not answer any question, unless entry into a program requires it
 - Client has the right to know who has added to, deleted, or edited their ServicePoint record
 - Information that is transferred over the web is through a secure connection
- 5. Benefits for clients**
 - Case manager tells client what services are offered on site or by referral through the assessment process
 - Case manager and client can use information to assist clients in obtaining resources that will help them find and keep permanent housing.

Written Client Consent

Each Client whose record is being shared electronically with another Partner Agency must agree via a written client consent form to have their data shared. A

client must be informed as to what information is being shared and with whom it is being shared.

Unnecessary Solicitation: The Participating Agency will not solicit or input information from clients unless it is essential to provide services, or conduct evaluation or research.

Sever access: The Participating Agency understands that BIS will maintain the server, which will contain all client information. All client identifiable data is inaccessible to unauthorized users.

(SYSTEM ADMINISTRATORS)

Policy:	All data will be handled according to the following major classifications: <i>Confidential Data</i> or <i>Open Data</i> . BIS and WISP staff will assess all data and implement appropriate controls to ensure that data classified as open and confidential data are handled according to the following procedures.
----------------	--

Procedures: WISP staff will administer the categories of data by adhering to the type of controls required for enforcing and maintaining security standards.

Definitions:

The classifications for these two types of data subsets are mutually exclusive. Therefore, for any given set that has any confidential data shall be considered confidential.

- *Open Data* – Unrestricted information that contains no data elements that are or could be used as personal identifiers. This type of data tends to statistical summaries of confidential data sets or counts of services.
- *Confidential Data*- Information that identifies clients contained within the database. Examples include social security number, name, address, or any other information that can be leveraged to identify a client.

Procedures for transmission and storage of data:

- *Open Data:* Data is subject to further classification (*see Open Data – Assessment and Access*) and scrutiny depending on the intent for the data and its audience. Unless this data is further classified as Public Data, then it should be handled discretely..
- *Confidential Data at the System Level:* As a system administrator in the normal course of assisting agencies staff may handle confidential information. Additionally confidential data may be used for internal analysis or in the preliminary process of creating open data. Whenever confidential data is accessed:
 - ✓ Hard copies shall be shredded when disposal is appropriate.
 - ✓ Hard copies shall be stored in a secure environment such that is inaccessible to the general public or staff who do not require access. This may include the following: locked file drawers, in employee's physical possession and control like in a briefcase.
 - ✓ Hard copies shall not be left out in the open or unattended.
 - ✓ Electronic copies shall be stored only where the employee can access the data.
 - ✓ Electronic copies shall be stored where a password is required to access the data if on shared server space.
 - ✓ Electronic copies shall be stored in the employee's physical control like on a diskette, CD-ROM, or a personal computer accessed only by the employee.

All data must be classified open or confidential and failure to handle data properly is a violation of this policy

Violations of these work rules as well as violations of statutes or administrative codes will result in appropriate disciplinary actions.

Policy: All data will be handled according to the following major classifications: *Confidential Data* or *Open Data*. BIS and WISP staff will assess all data and implement appropriate controls to ensure that data classified as open and confidential data are handled according to the following procedures.

Procedures: WISP staff will administer the categories of data by adhering to the type of controls required for enforcing and maintaining security standards.

Definitions:

The classifications for these two types of data subsets are mutually exclusive. Therefore, for any given set that has any confidential data shall be considered confidential.

- *Open Data* – Unrestricted information that contains no data elements that are or could be used as personal identifiers. This type of data tends to statistical summaries of confidential data sets or counts of services.
- *Confidential Data*- Information that identifies clients contained within the database. Examples include social security number, name, address, or any other information that can be leveraged to identify a client.

Procedures for transmission and storage of data:

- *Open Data:* Data is subject to further classification (see Open Data – Assessment and Access) and scrutiny depending on the intent for the data and its audience. Unless this data is further classified as Public Data, then it should be handled discretely. These data must be stored out of site and can be transmitted via internal or first-class mail until it is considered public data.
- *Confidential Data* at the Agency Level: Each agency shall promulgate rules governing the access of confidential data in WISP, ensuring that those staff needing to do so can access the data while restricting the access of those staff not needing access. The agency rules shall also cover the destruction of paper and electronic data in a manner that will ensure that privacy is maintained and that proper controls are in place for the hard copy and electronic data that is based on WISP data.

Note: For assistance in creating an Agency –wide IT policy see Entech’s [“Nonprofit Technology Policy Template.”](#)

All data must be classified open or confidential.

Public data may never include confidential data.

All data must be handled according to its classification.

Failure to handle data properly is a violation of this policy and violators will be subject to statutes and administrative code.

Wisconsin ServicePoint 3.X
Standard Operating Procedures

DATE
02/16/2004

SECTION
2.3

REVIEWER
TW

OPEN DATA - ASSESSMENT AND ACCESS

Policy: All open data will be handled according to the following classifications: *Public Data*, *Internal Data*, *Restricted Data*. WISP and Agency staff will assess all data and implement appropriate controls to ensure that data classified as public

domain data, internal data, restricted data and confidential data are handled according to the following procedures.

Procedures: Each agency will administer the categories of data that BIS and WISP staff will delineate by adhering to the type of controls required for enforcing and maintaining security standards.

Definitions:

The classifications of data are not mutually exclusive. Therefore, for any given data set (*whether in hard or electronic form*) the most restrictive security and confidentiality protocol applies.

- *Public Data*- Information from WISP that is shared with the general public in either written, electronic or verbal format
- *Internal Data*- Information scheduled, but not yet approved, for publication. Examples include draft reports, fragments of data sets, or data without context.
- *Restricted Data*- Information that has been created or accessed primarily for administrative purposes. This data may or may not eventually be made public.

Procedures for transmission and storage of data:

- *Public Data*: Security controls are not required but the data may not include any client identifiers such that an individual could be identified even through inference. The data shall reasonably reflect the elements from which it was derived in WISP and shall identify constraints or inferences related to its use or generalizability.
- *Internal Data* is accessible only to internal employees. No auditing is required. No special requirements around destruction of these data are required. These data must be stored out of site and can be transmitted via internal or first-class mail.
- *Restricted Data*: Need to know access only. Requires auditing of access and must be stored in a secure location. There are not special requirements around destruction of these data. If mailed internally must be labeled confidential; can be mailed first class.

All open data must be classified public, internal, restricted, or confidential.

Public data may never include confidential data.

All data must be handled according to their classification.

Failure to handle data properly is a violation of this policy.

SECURITY – BOWMAN INTERNET SYSTEMS (BIS)

Policy: Access to all of central server computing, data communications and sensitive data resources will be controlled. Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers. Access control violations must be

monitored, reported and resolved. BIS staff will work to ensure that all sites receive the security benefits of the system while complying with all stated policies. Security for WISP is contained in four areas: Application Security, Over the Wire/Network Security, Database Security, and HIPAA/Security Policies.

Procedure:

Physical Security

Bowman Internet Systems' data center is located at its headquarters in Shreveport, Louisiana. Located in a 20-story office complex, 24-hour security is provided. After normal business hours, card access is required and monitored. In addition, separate, limited key access is required for entry into the main office and into the server room.

Firewall Protection

The first step in protecting a network is to provide firewall protection. BIS secures the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

SSL Data Encryption

BIS utilizes commercial-grade, 128-bit SSL encryption from security leader, Verisign (www.verisign.com), for data traveling over the Internet to BIS's network. As a user enters ServicePoint™, they access data with 128-bit encryption from their browser and 1024-bit RSA public key from the ServicePoint servers. Distinguished by a lock icon in the corner of their browser, users are ensured that their data is secure in transit.

User Authentication

ServicePoint™ can only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. If a user enters an invalid password four consecutive times, ServicePoint™ automatically shuts them out of that session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security

In addition to restricting access to only authorized users, ServicePoint™ utilizes a system of multiple access levels. These levels automatically detect the user access level and controls access to appropriate data.

Database Security

Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Wisconsin ServicePoint 3.X
Standard Operating Procedures

DATE
02/16/2004

SECTION
2.5

REVIEWER
TW

SECURITY– DIVISION OF COMMUNITY DEVELOPMENT – –SYSTEM ADMINISTRATORS –

Policy: Access to all of computing, data communications and sensitive data resources will be controlled. Access is controlled through user identification and authentication. System Administrators are responsible and accountable for

work done under their personal identifiers. Access control violations must be monitored, reported and resolved. BOH staff will work to ensure that all sites receive the security benefits of the system while complying with all stated policies.

Procedure:

Physical Security

WISP is part of the Bureau of Housing and is located at its headquarters at the Department of Commerce. Located in an 8-story office complex, off-business hour security is provided. After normal business hours, card access is required and monitored. In addition, passwords are required to access individual workstations.

System Access Monitoring

WISP automatically tracks and records access to every client record by use, date, and time of access. WISP staff at Commerce will monitor access to system software. WISP staff will regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access. WISP will audit all unauthorized accesses and attempts to access information. Audit records shall be kept at least six months.

Media and Hardcopy Protection

[\(See Confidential And Open Data– Division Of Community Development\).](#)

User Authentication

WISP will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. If an administrator enters an invalid password four consecutive times, WISP automatically shuts them out of that session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Administration and System-wide Data

System Administrator II's will have full access to WISP, can add, edit and delete users, agencies, and programs and can reset passwords. Access to system-wide data will be granted based upon need to access the data and with the approval of the steering committee. The number of staff with a System Administrator II designation will be limited to as few as possible.

Data Security

Wherever possible, all database access is controlled at the operating system and database connection level for additional security.

Wisconsin ServicePoint 3.X
Standard Operating Procedures

DATE
02/16/2004

SECTION
2.6

REVIEWER
TW

SECURITY– SYSTEM ADMINISTRATOR Access –

Policy: As System Administrators have access to virtually all data contained in WISP, additional screening precautions are needed prior to their being designated System Administrator.

Procedure:

Screening and review Process

The following steps are to be integrated into the process of designating an individual as a WISP System Administrator I or II. These steps are to be completed prior to the individual receiving that level of authority.

1. The Departmental Human Resources (HR) staff would be given the name of an employee or applicant being considered as a System Administrator; (the employee would need to sign any required releases for this request)
2. HR would contract with an appropriate party for a criminal background check, reviewing state and federal court records. In addition, HR will review the employees State of Wisconsin personnel file for items which could potentially impact on the performance of the employee in this role.
3. The Director of the Bureau of Human Resources, the Departments General Counsel, and the Director of the Bureau of Housing are to discuss any findings in either the criminal background check or the employee personnel file that may be of concern.
 - The Director then reviews the material, discussing any potential concerns with the employee, and if satisfied with the individual, the Bureau Director will sign a form indicating that this review has been completed thereby authorizing that the individual is eligible for access to WISP, with system administrator status;
4. The authorization form is placed in a folder maintained by the Bureau with all other employee access statements.
5. Once approved, the employee also must sign a confidentiality agreement indicating that they are aware that information in WISP is to be considered confidential and treated as such and it thereby bound to the Department personnel rules related to confidential information.

The Bureau of Housing is to maintain a folder with all of the above mentioned documents in a confidential manner.

Related Documents

WISP Confidentiality Agreement. This document is to be signed by all WISP system administrators, level I and level II. Within this form the employee acknowledges that the WISP database is considered confidential information and as such is subject to the code of ethics which is administered by the Office of Employment Relations, as authorized by Chapter 19 of the Wisconsin Statutes. The Code of Ethics may be found in Chapter ER-MRS 24 of the Wisconsin Administrative Code.

Access Permission. This form, signed by the Director of the Bureau of Housing, specifies that the required criminal check and employee personnel file have been reviewed, and that the Director is hereby granting permission for the employee to have access to WISP confidential information as a system administrator.

SECURITY – Virtual Private Network (VPN)

Policy: Access to the Virtual Private Network connection to the WISP database will be restricted to those having System Administrator 2 level access in WISP and the responsibility of doing system level data analysis and reporting where Access will be limited to read only and may not include information subject to HIPPA regulation if client identifiers are accessed.

Only the IT System Administrator will have access to changing information in the database at the server level.

Procedure

Reporting

The VPN may be used to allow System Administrator 2 direct access to the database to facilitate reports and analysis with report generating software such as Crystal Reports. This access to the database is read only.

Data Changes

Where it necessary and appropriate, the IT staff, having System Administrator 2 authorization, may use the VPN connection to make changes in the database. When this is done and appropriate written summary of the information changed will be logged.

SECURITY – PARTNER AGENCIES

Policy:	Access to all of computing, data communications and sensitive data resources will be controlled. Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers. Access control violations must be monitored, reported and resolved. Agency staff will work to ensure that all sites receive the security benefits of the system while complying with all stated policies.
----------------	---

Procedures:

Physical Security

Agencies must develop rules to address unattended workstations and physical access to workstations. Monitors displaying client data should be oriented to minimize viewing by unauthorized people.

Access to Data

- A. User Access:** Users will only be able to view the data entered by users of their own agency or shared client records. Security measures exist within the WISP software system which restrict agencies from viewing each other's data.
- B. Raw Data:** Users who have been granted access to the WISP Report Writer tool have the ability to download and save client level data onto their local computer. Once this information has been downloaded from WISP in raw format to an agency's computer, these data then become the responsibility of the agency. A Partner Agency must develop protocol regarding the handling of data downloaded from Report Writer, record disclosure and storage.
- C. Agency Policies Restricting Access to Data:** Each Partner Agency must establish internal access to data protocols. These policies should include who has access, for what purpose, user account sharing and how they can transmit this information. Other issues to be addressed include storage, transmission and disposal of these data. [See Access Levels for System Users.](#)

Media and Hardcopy Protection

[\(See Confidential And Open Data–Partner Agencies\).](#)

User Authentication

WISP will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. If a user enters an invalid password four consecutive times, WISP automatically shuts them out of that session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals. WISP log-on IDs and passwords are never reset or established in the same communication. [See Access Privileges to System Software.](#)

ACCESS LEVELS FOR SYSTEMS USERS

Policy:	Partner Agencies will manage the proper designation of user accounts to enforce aforementioned information security protocols.
----------------	--

Procedure: User accounts will be created and deleted by the agency administrator under the authorization of the agency's executive director. Users will be given various access levels.

Access Levels

Resource Specialist I – Under this access level, a user may access only the ResourcePoint module. Users may search the database of area agencies and programs and view the agency or program detail screens. Access to client or service records and other modules and screens is not given. A resource specialist cannot modify or delete data.

Resource Specialist II – Under this access level, a user may access only the ResourcePoint module. Users may search the database of area agencies and programs and view the agency or program detail screens. Access to client or service records and other modules and screens is not given. A Resource Specialist II is an agency-level "Information & Referral (I&R) specialist" who may update their own agency and program information.

Resource Specialist III – Under this access level, a user may access only the ResourcePoint module. Users may search the database of area agencies and programs and view the agency or program detail screens. Access to client or service records and other modules and screens is not given. A Resource Specialist III may edit the system-wide news feature of WISP.

Volunteer – Under this access level, a user may access ResourcePoint, and have limited access to ClientPoint, and to service records. A volunteer may view or edit basic demographic information about clients (the profile screen), but is restricted from all other screens in ClientPoint. A volunteer may also enter new clients, make referrals, or check-in/out a client from a shelter. A volunteer does not have access to the "Services Provided" tab in WISP. Normally, this access level is designed to allow a volunteer to perform basic intake steps with a new client and then refer the client to an agency staff or case manager.

Agency Staff – Under this access level, a user may access ResourcePoint, and have full access to service records, but only limited access to ClientPoint. Agency staff may access most functions in ServicePoint, however, they may only access basic demographic data on clients (profile screen). All other screens are restricted including Reports. Agency Staff can add news items to the newswire feature of ServicePoint.

Case Manager I – Under this access level, a user may access all WISP screens and modules except "Administration." A Case Manager I may access all screens within ClientPoint except, for confidentiality reasons, the medical screen. They also may access Reports.

Wisconsin ServicePoint 3.X
Standard Operating Procedures

DATE
02/16/2004

SECTION
2.9 (1)

REVIEWER
TW

Case Manager II – Under this access level, a user may access all WISP screens and modules except "Administration." A Case Manager II may access all screens within ClientPoint, including the medical screen. They also may access Reports.

Agency Administrator – Under this access level, a user may access all ServicePoint screens and modules. This level may add/remove users and edit agency and program data for his/her agency.

Executive Director – same access rights as Agency Administrator, but ranked above Agency Administrator.

System Operator – Under this access level, a user may just access “Administration.” The system operator can setup new agencies, add new users, reset passwords, and access other system-level options. The system operator may order additional user licenses and modify the allocation of licenses. They maintain the system, but may not access any client or service records.

System Administrator I– same access rights to client information as Agency Administrator, but not for all agencies in the system. Also has full access to administrative functions

System Administrator II– No restrictions. Full access to WISP.

	Resource Specialist I	Volunteer	Agency Staff	Case Manager I	Case Manager II	Resource Specialist II	Agency Administrator	Executive Director	Resource Specialist III	System Operator	System Administrator I	System Administrator II
ClientPoint												
Profile		X	X	X	X		X	X			X	X
Medical/Addiction					X		X	X			X	X
Residential, Employment, Military/ Legal, Case Management, Case Notes and Worksheet History				X	X		X	X			X	X
ServicePoint												
Referrals		X	X	X	X		X	X			X	X
Services Provided			X	X	X		X	X			X	X
ResourcePoint	X	X	X	X	X	X	X	X	X	X	X	X
ShelterPoint		X	X	X	X		X	X			X	X
Reports				X	X		X	X			X	X
Administration												
Add/Edit Users							X	X		X	X	X
Reset Password							X	X		X	X	X
Add Agency									X	X	X	X
Edit Agency						X	X	X	X	X	X	X
Delete Agency									X	X	X	X
Add/ Edit/ Delete Programs						X	X	X	X	X	X	X

Wisconsin ServicePoint 3.X
Standard Operating Procedures

DATE
02/16/2004

SECTION
2.9 (2)

REVIEWER
TW

ACCESS PRIVILEGES TO SYSTEM SOFTWARE

Policy: Partner Agencies will apply the user access privilege conventions set forth in this procedure.

Procedure: Allocate user accounts and privileges according to the format specified as follows:

User Access Privileges to WISP

- A. User access:** User access and user access levels will be determined by the executive director of the participating agency in consultation with the system administrator. The system administrator will generate a username and password for the agency administrator who will, in turn, then generate usernames and passwords for agency users.
- B. Agency Administrator Qualifications:** Time, interest, and ability are the biggest factors in determining who should be an Agency Administrator. This title does not necessarily correspond to the agency's organizational chart. The user designated as the Agency Administrator may also enter client data.
- C. Passwords:**
 - 1. Creation:** Passwords are automatically generated from the system when a user is created. Site technical administrators will communicate the system-generated password to the user.
 - 2. Use of:** The user will be required to change the password the first time they log onto the system. The password must be between 8 and 16 characters and contain 2 numbers. Passwords are the individual's responsibility and users cannot share passwords. Passwords should not be easily guessed or found in any dictionary and should be securely stored and inaccessible to other persons. The password is alphanumeric.
 - 3. Expiration:** Passwords expire every 45 days. A password cannot be re-used until one entirely different password selection has expired.
 - 4. Termination or Extended Leave from Employment:** The Agency Administrator should terminate the rights of a WISP user immediately upon termination from their position. If a staff person is to go on leave for a period of longer than 45 days, their password should be inactivated within 5 business days of the start of their leave. The Agency Administrator is responsible for removing users from the system.

ANONYMOUS CLIENTS

Policy: For **domestic violence clients and their households only**, when a client and feels that entry of his/her name and the names of the members of their households into WISP present an immanent threat to their safety, the client and their household may be added anonymously. When entering a client anonymously, it is incumbent upon the agency to keep a record of the client's unique anonymous I.D. to avoid duplication of entry.

Procedure:

Add a client to WISP without entry of his/her name by using WISP's Anonymous Client feature. When this feature is used, WISP generates a code number for the client record that the agency maintains in a secure location along with the person's name. The only way to access the client record is to use the code number.

The following is a list of required actions a domestic violence agency must do when using the anonymous client feature:

- A. Enter the client's gender and date of birth. This ensures that aggregate reports detail the correct number of males vs. females and adults vs. children served
- B. If the client feels that entry of the actual birth date is too identifying, domestic violence agencies may use 01/01/yyyy for the birth date where yyyy is the actual birth year.
- C. Keep a record of this client's anonymous I.D. on file. The unique ID is found in the Last name field on the Profile screen. You will need the unique ID to retrieve the client record.

Creating anonymous records may mean that your reports will not provide a true unduplicated count and therefore this option should only be used if absolutely necessary.

RELEASE OF INFORMATION (ROI)

Policy	A client must give permission for personal data to be shared with other agencies in WISP. A client does not need to give permission for information to be shared within an agency. For minors, a parent or guardian must also give permission for their child's data to be shared.
---------------	--

Paper Release of Information

Procedure: Every client must be given an opportunity to sign a paper copy of a release of information for their data that will be input into Wisconsin ServicePoint software . These releases must then be filed at the agency. Only one paper copy of a release of information is required per agency, this release could then cover all programs within an agency.

Software Release of Information

Procedure: Every client must have a ROI attached to their profile in the software and this ROI must be established prior to filling out any assessment information in every single program that a client enters. Regardless of the intent of the client, always indicate that a release was granted. The recommended length for the ROI is three years.

A client permits open access to his or her records or agrees to the default settings of the agency and signs a release to that effect. The user would indicate that a release was granted and that there is a “Signed Statement from the Client.”

A client does not permit the release of his or her information but the program still intends to share the information within the agency. The user would indicate that a release was granted and that the type of release is “None”. To close the client’s records to outside agencies while still keeping the information available within the agency requires either of the following steps:

Option A: If the client has just been created, then go to the security lock in the right-hand corner of the screen in the orange bar and click the client’s record to close. Then check each of your programs in the possible exceptions to ensure that each will still have access to the data

Option B: If the client is already in the system but now wants future information closed, then go into each individual assessment and click on the security lock and change the record to close. Then check each of your programs in the possible exceptions to ensure that each will still have access to the data.

A client calls a central point of intake and agrees to release the information to the referring agencies. The user would indicate that a release was granted and that there was Verbal Consent. The program profile would be set-up such that the release only allowed information to flow to the other programs in the agency or to those programs for which the central point of intake has an agreement.

Wisconsin ServicePoint 3.X	DATE	SECTION	REVIEWER
Standard Operating Procedures	02/16/2004	2.12	TW

Data Expectation and System Usage

Section 3

Data Collection Protocol	3.1
Assessment Setup	3.2
Data Integrity and Reliability	3.3
Default Restrictions and Exceptions	3.4

DATA COLLECTION PROTOCOL

Policy:	Partner Agencies that collect client data through WISP will agree to collect the prescribed data elements. These elements will ensure that data collected by the agencies will be useful for measuring program usage and drawing inferences. The requirements will be derived from the Data Standards promulgated by HUD and from recommendation by the Wisconsin ServicePoint Steering Committee.
----------------	--

Procedure: The Partner Agency is responsible for committing to and ensuring that all clients are asked a minimal set of questions for use in aggregate analysis. These questions are included in custom assessments, created by WISP System Administrators. The required data elements are dependent on the program. Additionally, with each assessment the mandatory data elements are displayed in RED text and/ or specific text indicating that the field is required. The Partner Agency agrees to minimally enter this level of information into WISP.

The agency administrator must identify the assessments and requirements for each program and properly set-up each program in WISP.

AGENCY PROFILE ASSESSMENT SETUP

Policy: The following Assessments should be set-up accordingly.

Procedure:

Agency Program Type	Show on Profile	Show on ENTRY	Show on EXIT	Assessments that Must be visible
Emergency Shelter	WI Assessment	N/A	N/A	WI Additional Profile & WI Medical Assessment
Transitional Shelter	WI Assessment	N/A	N/A	Additional Profile WI Medical Assessment
Safe Haven	WI Medical Assessment	WI Assessment	WI Exit Assessment	Additional Profile
Transitional Housing (Includes non-DHIR & DHIR funded)	WI Medical Assessment	WI Assessment	WI Exit Assessment	Additional Profile
Supportive Housing Program	WI Medical Assessment	WI Assessment	WI Exit Assessment	Additional Profile
Permanent Supported Housing	WI Medical Assessment	WI Assessment	WI Exit Assessment	Additional Profile
Rental Assistance	WI Medical Assessment	WI Assessment	WI Exit Assessment	Additional Profile
Motel Voucher	WI Medical Assessment	WI Assessment	N/A	Additional Profile
WI Call- In/Screening	WI Call-In Assessment	WI CI Assessment On Entry	N/A	Additional Profile WI Medical
WI Food Pantry	WI Food Pantry Assessment	WI FP On Entry	N/A	WI Medical Assessment & WI Additional Profile
Services (none of the above)	WI Assessment	WI Assessment	N/A	WI Medical Assessment & WI Additional Profile

All programs in all agencies will see and use the following:

Profile – which shows the clients name, social security number, and displays the age

Household – this sub-assessment type question will record the household type, the relationship of the client in the household, and indicate if the client is the head of household

WI Additional Profile – this assessment, selected from the visible assessment listing, includes the client: dob, gender, race, ethnicity, drivers license number, city and state of birth. It includes both optional and mandatory fields.

DATA INTEGRITY AND RELIABILITY

Policy:	WISP staff will occasionally monitor the prevalence of data collection for random variables and hold participating agencies accountable. WISP Partner agencies are responsible for the overall quality, accurateness, and completeness of data entered by their staff for their clients.
----------------	--

Procedure:

Standards for minimum level of participation by partner agencies will be established. Then periodically, system administrator's will run system-wide reports to assess the quality and level of participation by partner agencies. Statistical results of these surveys will be shared with partner agencies.

Wisconsin ServicePoint 3.X	DATE	SECTION	REVIEWER
Standard Operating Procedures	02/16/2004	3.3	TW

DEFAULT RESTRICTIONS AND EXCEPTIONS

Policy:	WISP staff will establish basic requirements for assessment administration in the “Default Restrictions and Exceptions” box in the profile program set-up in WISP Administration, such that agencies will be allowed the greatest amount of flexibility while ensuring that the potential for duplicate entries for one client is as minimal as possible.
----------------	---

Procedure:

In the “Admin Provider” profile in the Administration screen in WISP in “Default Restrictions and Exceptions” where the agency administrator has the option to keep data entered into a program either open or closed the following must remain open: “*Client*” and “*WI Additional Profile*.”

The only exception to this rule is for programs that serve victims of domestic violence, runaway youth, individuals with HIV or AIDS and those with AODA issues. For these types of programs, it would be permissible to close “*Client*” and “*WI Additional Profile*” as default in the provider profile page.

Individual client records could still be closed at the client’s request in the actual record itself in ClientPoint.